

AO 106 (Rev. 04/10) Application for a Search Warrant

FILED

ENTERED

LODGED

RECEIVED

AUG 09 2018

## UNITED STATES DISTRICT COURT

for the

Western District of Washington

AT SEATTLE  
CLERK U.S. DISTRICT COURT  
WESTERN DISTRICT OF WASHINGTON  
DEPUTY  
BY

In the Matter of the Search of

(Briefly describe the property to be searched  
or identify the person by name and address)

Subject devices in the custody of U.S. Secret Service,  
further described in Attachment A

Case No.

MJ18-363

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

Subject devices as further described in Attachment A, which is attached hereto and incorporated herein by this reference.

located in the Western District of Washington, there is now concealed (identify the person or describe the property to be seized):

See Attachment B, which is attached hereto and incorporated herein by this reference.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
Title 18 USC 371, 1349	Conspiracy
Title 18 USC 134	Wire Fraud
Title 18 USC 1029	Access Device Fraud

The application is based on these facts:

See Affidavit of United States Secret Service Special Agent Yoshiko Marinko, attached hereto and incorporated herein by reference.

☒ Continued on the attached sheet.

☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

  
Applicant's signature

Special Agent Yoshiko Marinko

Printed name and title

Sworn to before me and signed in my presence.

Date: 8-9-18

City and state: Seattle, Washington

  
Judge's signature

Paula L. McCandlis, United States Magistrate Judge

Printed name and title

**ATTACHMENT A**

**SUBJECT DEVICES TO BE SEARCHED**

- (a) Lenovo Laptop, Black; Serial # CB18751780; Model G585
- (b) Acer Laptop, Black; Serial # NXGFTAA0117020D2253400; Model # N16C1
- (c) Moto Cell Phone; Model XT1687; Serial # Inaccessible
- (d) Huawei Honor Cell Phone; Model BLN-L24; Serial # Inaccessible
- (e) Sandisk Flash Drive, 32 GB; BM170525665Z
- (f) Transcend Flash Drive, 4GB; N14939
- (g) Samsung Galaxy S9+ phone, Black; Serial # R38K30T7Q2Z; IMEI:  
343321092412611

All of the aforementioned items or devices are currently in the custody of the  
United States Secret Service, located in Seattle, Washington

**ATTACHMENT B**  
**ITEMS TO BE SEIZED**

All evidence on the SUBJECT DEVICES described in Attachment A that constitutes fruits, contraband, evidence and instrumentalities of violations of 18 U.S.C. §§ 371 and 1349 (Conspiracy), 18 U.S.C. § 1029 (Access Device Fraud), 18 U.S.C. § 1343 (Wire Fraud) (collectively, the "Subject Offenses"), for the time period of **January 1, 2017 to December 1, 2017**, including:

a. Documents, records or files relating to the identification of the individuals committing the Subject Offenses

b. Documents, records or files relating to credit/debit card, gift card, or account or card numbers;

c. Documents, records or files relating to planned, attempted, or successful use of gift cards or card data to conduct purchases or transactions;

d. Documents, records or files relating to the purchase, receipt, manufacture, maintenance, or use of card-reading or encoding equipment or software, device-making equipment;

e. Documents, records or files relating to the creation, manufacture, possession, transfer, or use of counterfeit cards or stolen card data, including the Luhn algorithm software or files that may be used for encoding and/or re-encoding gift cards;

f. Documents, records or files relating to or referencing Target, transactions conducted at Target, items or services purchased from Target, or communications about Target or with Target representatives;

g. Documents, records or files relating to online vendors, such as Paxful, where gift cards and gift card balances may be listed, sold, or purchased;

h. Documents, records or files relating to cryptocurrency, such as Bitcoin, and the use and possession thereof, including any wallets and passcodes and public/private keys thereto;

i. Documents, records or files indicating dominion and control;

1 j. Documents, records or files relating to the deposit, withdrawal, or transfer  
2 of funds, including, but not limited to, wire transfers;

3 k. Photographs depicting cash, cards/card stock, device-making equipment,  
4 transactions, and/or any other individual that may be involved in the criminal scheme;

5 l. Documents, records or files establishing criminal associations, including  
6 address books, contact lists, and telephone or communication records;

7 m. Documents, records or files relating to software, programs or applications,  
8 such as Pocket Zee, that enables the use of gift cards or gift card numbers on digital  
9 devices;

10 n. Documents, records or files relating to the use or sale of items purchased  
11 using stolen Target gift card numbers;

12 o. Evidence of user attribution showing who used or owned the SUBJECT  
13 DEVICES at the time the things described in this warrant were created, edited, or deleted,  
14 such as logs, phonebooks, contact lists, saved usernames and passwords, documents,  
15 pictures/photographs, and browsing history;

16 p. Records and/or data that may reveal the past location of the individual or  
17 individuals using the SUBJECT DEVICES;

18 q. Any passwords, password files, test keys, encryption codes or other  
19 information necessary to access computer equipment, storage devices or data.

20 r. For each of the SUBJECT DEVICES:

21 i. Evidence of who used, owned, or controlled the digital device or  
22 other electronic storage media at the time the things described in this warrant were  
23 created, edited, or deleted, such as logs, registry entries, configuration files, saved  
24 usernames and passwords, documents, browsing history, user profiles, email, email  
25 contacts, "chat," instant messaging logs, photographs, and correspondence;

26 ii. Evidence of software that would allow others to control the digital  
27 device or other electronic storage media, such as viruses, Trojan horses, and other forms  
28

1 of malicious software, as well as evidence of the presence or absence of security software  
2 designed to detect malicious software;

3           iii.       Evidence of the lack of such malicious software;

4           iv.       Evidence of the attachment to the digital device of other storage  
5 devices or similar containers for electronic evidence;

6           v.        Evidence of counter-forensic programs (and associated data) that are  
7 designed to eliminate data from the digital device or other electronic storage media;

8           vi.       Evidence of the times the digital device or other electronic storage  
9 media was used;

10          vii.       Passwords, encryption keys, and other access devices that may be  
11 necessary to access the digital device or other electronic storage media;

12          viii.      Documentation and manuals that may be necessary to access the  
13 digital device or other electronic storage media or to conduct a forensic examination of  
14 the digital device or other electronic storage media;

15          ix.        Contextual information necessary to understand the evidence  
16 described in this attachment.

17  
18  
19        As used above, the terms “documents,” “records,” and “information” include all of  
20 the foregoing items of evidence in whatever form and by whatever means they may have  
21 been created or stored, including any form of computer or electronic storage (such as  
22 flash memory or other media that can store data) and any photographic form.  
23  
24  
25  
26  
27  
28

**AFFIDAVIT**

STATE OF WASHINGTON )

) ss

COUNTY OF KING )

I, Yoshiko Marinko, being first duly sworn on oath, depose and say:

**INTRODUCTION AND AGENT BACKGROUND**

1. I am a Special Agent (SA) with the United States Secret Service (USSS) and have been so since August 27, 2001. I am currently assigned to the Seattle Field Office.

2. I am a graduate of the Federal Law Enforcement Training Center (FLETC) located in Glynnco, Georgia, and the Secret Service Special Agent Training Program located in Beltsville, Maryland. As part of my training with the Secret Service, I have received instruction on the investigation of financial crimes, including credit/debit card fraud, mail and wire fraud, access device fraud, and identity theft. In the course of my law enforcement career, I have investigated crimes ranging from the production and passing of counterfeit currency, identity theft, access device fraud, bank fraud and threats made against the President and Vice President of the United States. I have a Bachelor of Science degree from the United States Air Force Academy and a Master of Science degree from Troy State University.

3. I am familiar with, and have participated in, a variety of investigative techniques including, but not limited to, analysis of documentary and financial evidence, surveillance, the questioning of witnesses, the implementation of undercover operations, and execution of search and seizure warrants.

//

//

1           4. I make this Affidavit in support of an application under Rule 41 of the  
 2 Federal Rules of Criminal Procedure for a warrant to search the following digital devices<sup>1</sup>  
 3 and other electronic storage media<sup>2</sup> (hereinafter "SUBJECT DEVICES"), as more fully  
 4 described in ATTACHMENT A to this Affidavit, for the items described in  
 5 ATTACHMENT B to this Affidavit, which are incorporated herein by reference:

6           (a) Lenovo Laptop, Black; Serial # CB18751780; Model G585

7           (b) Acer Laptop, Black; Serial # NXGFTAA0117020D2253400; Model #  
 8 N16C1

9           (c) Moto Cell Phone; Model XT1687; Serial # Inaccessible

10          (d) Huawei Honor Cell Phone; Model BLN-L24; Serial # Inaccessible

11          (e) Sandisk Flash Drive, 32 GB; BM170525665Z

12          (f) Transcend Flash Drive, 4GB; N14939

13          (g) Samsung Galaxy S9+ phone, Black; Serial # R38K30T7Q2Z; IMEI:  
 14 343321092412611  
 15

16          5. The facts set forth in this Affidavit are based on my own personal  
 17 knowledge; knowledge obtained from other individuals during my participation in this  
 18 investigation, including other law enforcement officers; review of documents and records  
 19 related to this investigation; communications with others who have personal knowledge  
 20 of the events and circumstances described herein; and information gained through my  
 21 training and experience.

22          6. Because this Affidavit is submitted for the limited purpose of establishing

23 \_\_\_\_\_  
 24 <sup>1</sup> "Digital device" includes any electronic device capable of processing and/or storing data in digital form, including,  
 25 but not limited to: central processing units, laptop or notebook computers, peripheral input/output devices such as  
 26 keyboards, printers, scanners, plotters, monitors, and drives intended for removable media, related communications  
 27 devices such as modems, cables and connections, and electronic/digital security devices wireless communication  
 28 devices such as telephone paging devices, beepers, mobile or cellular telephones, personal data assistants ("PDAs"),  
 iPods, blackberries, digital cameras, digital gaming devices.

<sup>2</sup> Electronic Storage media is any physical object upon which computer data can be recorded. Examples include  
 hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

1 probable cause in support of the application for a search warrant, it does not set forth  
2 each and every fact that I or others have learned during the course of this investigation. I  
3 have set forth only facts that I believe are sufficient to the determination of probable  
4 cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§  
5 371 and 1349 (Conspiracy), 18 U.S.C. § 1029 (Access Device Fraud), and 18 U.S.C. §  
6 1343 (Wire Fraud) (collectively, the "Target Offenses"), will be found on the SUBJECT  
7 DEVICES.

8 7. The requested warrant would authorize the forensic examination of the  
9 SUBJECT DEVICES for the purpose of identifying electronically stored information  
10 (ESI) particularly described in Attachment B.

11 8. The SUBJECT DEVICES are currently in the lawful possession of the  
12 United States Secret Service (USSS), located in Seattle, Washington, and were seized  
13 through the investigation, as described herein.

14 9. The SUBJECT DEVICES are currently in storage at the USSS evidence  
15 facility. In my training and experience, and based upon my involvement in this  
16 investigation, I know that the SUBJECT DEVICES have been stored in a manner in  
17 which their contents are, to the extent material to this investigation, in substantially the  
18 same state as they were when the SUBJECT DEVICES first came into the possession of  
19 law enforcement, as discussed below.

20 This Affidavit is being presented electronically pursuant to Local Criminal Rule  
21 CrR 41(d)(3).

#### 22 SUMMARY OF INVESTIGATION

23 10. As discussed in more detail below, this investigation relates to an elaborate  
24 fraudulent scheme that compromised the gift card system of a particular U.S. retailer,  
25 causing multiple hundreds of thousands of dollars (to date, at least approximately  
26 \$760,000) in loss. In short, a group of individuals, including Jeffery Mann and numerous  
27 others, some of whom are identified herein, reverse-engineered gift card numbers, which  
28 they used to make unauthorized purchases at various Target retail stores in the Western



1 District of Washington and elsewhere.

2 11. Target Corporation ("Target") began an investigation on or about June 8,  
3 2016, when Market Investigator Derek Forare became aware of fraudulent gift card  
4 activity impacting guests in Target stores in Western Washington. According to Forare,  
5 he was notified by Target's Lynnwood, Washington store team leader, Brandon Bogart,  
6 about possible fraud activity at the Lynnwood store. Bogart reported seeing suspicious  
7 transactions conducted by subjects over the preceding few days. These transactions  
8 involved multiple gift card numbers scanned from cell phones<sup>3</sup> to conduct high-dollar  
9 transactions.

10 12. Bogart had identified one of the subjects as "Jeremy" Mann who was  
11 involved with an incident at the store on April 20-21, 2017, involving a suspicious  
12 vehicle in the parking lot. He was later identified as Jeffery Mann through comparison of  
13 surveillance footage with his social media profile and communication with Lynnwood  
14 Police Department, which was aware of Jeffery Mann.

15 13. After receiving this information, Forare contacted Target's National  
16 Investigation Center and learned that Target had received several complaints in early  
17 June 2017 from customers who were missing balances from their Target gift cards, and  
18 Target was already working at corporate headquarters to investigate and gather  
19 information on the subjects involved in the fraud.

20 14. On June 10, 2017, Bogart (the Lynnwood store team leader) observed a  
21 group of four subjects attempt to make a \$900.00 purchase using gift cards on their cell  
22 phones at Target. Bogart was able to speak with the subjects in person at the cash  
23 register and provide guest service. Bogart immediately recognized one subject as Jeffery  
24 Mann from the previous incident at Target on April 21, 2017, and from the June 8, 2017,  
25 incident described above. The other male that was with Mann was identified as Corey  
26 Mosey, who had also been involved, and identified, in the April 21, 2017 suspicious  
27

28 <sup>3</sup> As described herein, in addition to traditional cards, gift card balances can be accessed and used through various electronic means, such as applications available on digital devices.

1 vehicle incident. In addition to Mann and Mosey, two females also accompanied them at  
2 the cash register. One female was later identified by Forare as Danielle Helm by  
3 matching her appearance on Target surveillance footage with images captured from her  
4 social media profiles. While Bogart talked with the subjects, he observed a mobile phone  
5 application open on the screen of one of their cell phones called "Pocket Zee."

6 According to Forare, Pocket Zee is a third-party mobile wallet application for a cell  
7 phone. It is unaffiliated with Target. The application allows a user to input a gift card  
8 number into the program, and creates a barcode image that can be scanned at Target  
9 registers at the time of purchase. Bogart denied the sale and the subjects exited the store.

10 15. On June 13, 2017, Forare was advised by the Bellingham, Washington store  
11 assets protection leader that individuals were observed at a Target store in Bellingham,  
12 Washington making purchases with multiple gift cards. Forare was able to match  
13 surveillance footage from Bellingham to the individual identified as Mann. According to  
14 Forare, Mann used several Target gift cards scanned from his cell phone to purchase an  
15 iTunes gift card.

16 16. According to Target investigators, including Forare and Target Special  
17 Investigator Alex Glistsos, the subjects involved in the fraud activity were not tampering  
18 with physical cards or taking photos of the barcodes in Target stores, as the compromised  
19 gift card balances included gift cards sold online at Target.com and those purchased by  
20 guests in other states throughout the country. Instead, the subjects had been able to  
21 decode the gift card numbers using something known as a Luhn algorithm, then create  
22 barcodes (using the third-party mobile wallet application) corresponding to the gift card  
23 numbers they obtained—numbers on gift cards that are sold or issued to guests every day.  
24 By doing this, the perpetrators were able to duplicate gift card barcodes without ever  
25 being in possession of the cards themselves. Target investigators also believed the  
26 subjects created gift card barcodes by starting with a known, working, gift card barcode  
27 and working backwards with the number sequence or algorithm, knowing that the  
28 previous gift card numbers had likely already been issued.

1           17. Based on information gathered on June 13, 2017, including surveillance  
2 and transaction records that included the names or emails of suspected perpetrators,  
3 Target's National Investigation Center was able to conduct social media searches and  
4 determine the identities of a number of subjects involved. The main group of subjects  
5 involved in the activity as of that date included: Jeffery Mann, Corey Mosey, Samantha  
6 Fleischacker, Kayle McCrary, Justin Brown, Danielle Helm, and Derrick Quintana.  
7 Connections to each other and their involvement in the gift card fraud were developed  
8 from observations of their joint presence in various stores where they conducted  
9 transactions with gift card numbers scanned from their phones, as well as pictures on  
10 social media showing subjects together.

11           18. On June 16, 2017, Forare contacted Detective Brad Reorda of the  
12 Lynnwood Police Department, and discussed the activity of Mann and the other subjects  
13 believed to be involved with Mann's fraudulent activity. According to Forare, Detective  
14 Reorda stated he was familiar with Mann and the other subjects, and explained that they  
15 are a transient group who are known to stay at different hotels.

16           19. On July 26, 2017, subjects Jeffery Mann, Derrick Quintana, and Lindsay  
17 Brandner were contacted by Marysville Police Department in a Motel 6 hotel room in  
18 Everett, Washington, during the unrelated arrest of a fourth individual also present in the  
19 room. According to police reports, officers identified a rented Jeep associated with the  
20 group, which Mann identified as belonging to him. Officers searched the hotel room and  
21 Jeep pursuant to warrants, and located gift card ledgers and worksheets, dozens of gift  
22 cards, including for Target, Steam.com, Hotels.com, and other retailers, a magnetic  
23 reader-writer, and financial paperwork and identifying documents belonging to third  
24 parties. Among the ledgers were lists of what Forare was able to recognize as Target gift  
25 card numbers, written in sequence, and notes taken on the card balances or descriptions.  
26 Among the notebooks, there was a note saying, "don't say anything about me teaching  
27 you b/c/ Jeff gets made cause he taught us." There were also notes related to the sale of a  
28 vehicle from "Kennady Weston" to another person, and the debt owed to "Kennady" as

1 of March 23, 2017.

2 20. Through its investigation, Target has identified and preserved surveillance  
3 footage of hundreds of transactions by individuals matching the physical characteristics  
4 of the subjects named in this Affidavit, including Jeffery Mann, Corey Mosey, Joshua  
5 Newman, Samantha Fleishacker, Derrick Quintana, Hayley Brown, Justin Brown,  
6 Danielle Helm, and numerous others. Based on Target records, these transactions  
7 typically involve the use of multiple gift card numbers to complete the purchase. As part  
8 of my investigation, I have reviewed such surveillance footage and records obtained from  
9 Target. In many instances, the footage shows the individual using that barcode scanner at  
10 the Target register on his or her cell phone. In some instances, the individual uses  
11 traditional (counterfeit) physical cards to conduct the transaction. Based on my training  
12 and experience, and that of other experienced investigators, I know that creating  
13 counterfeit cards often involves use of various digital devices, including computers,  
14 printers, and other devices.

15 21. On August 7, 2017, Forare emailed USSS that Mann and other subjects  
16 were travelling, and transactions at Target stores were made in Las Vegas, Nevada and  
17 Portland, Oregon in the last few days. Surveillance video from Target stores in the Las  
18 Vegas area in early August 2017 show transactions conducted by shoppers matching the  
19 physical attributes of subjects Jeffery Mann and Kennady Weston, using scans of cellular  
20 telephones to make purchases. Facebook posts from Derrick Quintana in August 2017  
21 show photos and videos of Quintana with individuals identified through social media  
22 profiles as Mann and Kennady Weston in what appears from the photos and videos to be  
23 Las Vegas. Records from Expedia show that, later in August 2017, the email address  
24 associated with Samantha Fleishacker's Facebook profile was used to book rooms in Las  
25 Vegas, with the registered guest identified as Derrick Quintana.

26 22. USSS learned that on August 5, 2017, three subjects—Corey Mosey, Kayle  
27 McCrary, and Timothy Brand—were arrested in Oregon by officers with the West Linn  
28 Police Department. According to police reports, Brand was arrested initially for DUI,

1 and officers discovered gift cards and other newly purchased merchandise with him (and  
2 passenger Mosey) in the car. Brand told officers that Mosey used the Luhn algorithm and  
3 the last few digits of a gift card number to see if the card was active or not. Brand  
4 admitted he (Brand) would go into Target stores and buy things with the fraudulent gift  
5 cards. Brand also identified Jeff Mann as the ringleader of the gift card operation and  
6 said that Mann was headed to Las Vegas (as noted above, Target Surveillance and social  
7 media posts show Mann in Las Vegas in early August 2017).

8 23. Officers obtained consent from Kayle McCrary and Corey Mosey to search  
9 the Motel 6 where they, and Brand, were staying. During the search they found Target  
10 gift cards with remaining balances written on the back, notebooks with apparent gift card  
11 numbers from various retailers. McCrary admitted to keeping records of the gift card  
12 numbers that were used, calling Target to determine balances, and transferring balances  
13 to applications on her cell phone.

14 24. The SUBJECT DEVICES described in Paragraph 4(a) through 4(e) of this  
15 Affidavit were located in either the car in which Mosey was a passenger at the time of  
16 Brand's arrest, or in the Motel 6 where Mosey, Brand and McCrary were staying. The  
17 evidence recovered in those searches, including these five SUBJECT DEVICES, were  
18 transported to the West Linn (Oregon) Police Department. That evidence was  
19 subsequently transferred to the possession of the USSS, and transported by USSS to  
20 Seattle, as described in Paragraph 29 of this Affidavit, below.

21 25. Each of Brand, Mosey, and McCrary were arrested and subsequently  
22 charged in Clackamas County Superior Court. Brand and McCrary resolved their cases  
23 with Clackamas County, while Mosey's case was still pending when the instant federal  
24 case was charged. It has subsequently been dismissed in favor of this federal  
25 prosecution.

26 26. On November 30, 2017, Kirkland Police Department (KPD) arrested  
27 Jeffery Mann in custody following an arrest for fraud. Along with KPD Detective  
28 Frankeberger, USSS SA Colby Garcia interviewed Mann. After waiving his *Miranda*

1 rights, Mann explained that he and his friend "Corey" had figured out that the barcodes  
2 for Target gift cards were determined by an algorithm. Using that algorithm (the "Luhn  
3 algorithm") enabled him to deduce what the gift card numbers for a given set or sequence  
4 of Target gift cards were likely to be. Mann said that Target was easy (or easier than  
5 some other retailers' gift cards) because it was only a barcode, and Target did not require  
6 an Access Number or PIN, and did not use random numbers. He explained that he and  
7 others participating in the scheme would get a gift card, scan it to get the numbers, and  
8 then work out the gift card numbers for other cards. He would call to check those  
9 numbers for fund balances, and then would add those numbers with a usable balance to  
10 his phone and make a barcode he could scan. Mann said he would then go to a Target  
11 store and purchase gift cards for Steam, Target, and other retailers. He would then re-sell  
12 these illegally purchased gift cards through online vendors, such as [www.paxful.com](http://www.paxful.com), in  
13 exchange for cryptocurrency, to include Bitcoin. Mann admitted to operating this scheme  
14 for the past six months (from roughly June 1, 2017) in several different states. He  
15 admitted doing it at multiple different Target stores in the metropolitan areas of each of  
16 Las Vegas, Denver, and Los Angeles, as well as an unknown number of stores in the  
17 greater Seattle area. Asked who else was involved, he said maybe 20 people he knows,  
18 and others that Corey Mosey knows. He gave the names of Hayley Brown, Kennady  
19 Weston and Derrick Quintana. Mann also estimated that he had personally profited over  
20 \$50,000.00.

21 27. Jeffery Mann was arrested and later charged in King County Superior  
22 Court. A number of digital devices, including several cellular telephones and laptops,  
23 were seized from Mann's car and hotel room at the time of his arrest. On May 11, 2018,  
24 the Honorable Brian A. Tsuchida signed a warrant authorizing the search of those digital  
25 devices. Subsequent to that warrant, one additional device, the SUBJECT DEVICE  
26 described at Paragraph 4(f) of this Affidavit, was discovered among the materials seized  
27 from Mann by Kirkland PD.

28 28. On May 31, 2018, a grand jury in the Western District of Washington



1 indicted Mann, Mosey, Weston, Quintana and Joshua Newman in a ten-count mail fraud  
 2 indictment for their fraud against Target described above. That case was assigned to the  
 3 Honorable James L. Robart under cause number CR18-136 JLR. Following the filing of  
 4 the federal indictment, the case against Mosey in Clackamas County, Oregon, and the  
 5 case against Mann in King County Superior Court, described above, were each dismissed  
 6 in favor of the federal prosecution. Mann, Mosey, and Newman have been arraigned on  
 7 the charges, and are in custody awaiting trial, which has been set for January 7, 2019.  
 8 Weston and Quintana have not yet been apprehended. At the time of his arrest,  
 9 Defendant Joshua Newman had in his possession the cellular telephone that is the  
 10 SUBJECT DEVICE described at Paragraph 4(g) of this Affidavit.

11 29. Following the dismissal of the Clackamas County case against Corey  
 12 Mosey, SA Carl Klein of the USSS Portland Field Office took possession of the evidence  
 13 related to that case being held at the West Linn Police Department on June 19, 2018. SA  
 14 Klein transported that evidence, including the SUBJECT DEVICES listed in Paragraph  
 15 4(a)-(e), to USSS in Seattle, where it has remained ever since.

#### 16 **DEFINITIONS AND TECHNICAL TERMS**

17 30. Set forth below are some definitions of technical terms, most of which are  
 18 used throughout this Affidavit pertaining to the Internet and computers generally. Based  
 19 on my training and experience, I use the following technical terms to convey the  
 20 following meanings:

21 a. **Computers and digital devices:** As used in this Affidavit, the terms  
 22 “computer” and “digital device,” along with the terms “electronic storage media,”  
 23 “digital storage media,” and “data storage device,” refer to those items capable of storing,  
 24 creating, transmitting, displaying, or encoding electronic or digital data, including  
 25 computers, hard drives, thumb drives, flash drives, memory cards, media cards, smart  
 26 cards, PC cards, digital cameras and digital camera memory cards, electronic notebooks  
 27 and tablets, smart phones and personal digital assistants, printers, scanners, and other  
 28 similar items.

1           b.     Wireless/cellular telephone: A wireless or cellular telephone (or  
2 mobile telephone) is a handheld wireless device used for voice and data communication  
3 through radio signals. These telephones send signals through networks of  
4 transmitter/receivers, enabling communication with other wireless telephones or  
5 traditional "land line" telephones. A wireless telephone usually contains a "call log,"  
6 which records the telephone number, date, and time of calls made to and from the phone.  
7 In addition to enabling voice communications, wireless telephones offer a broad range of  
8 capabilities. These capabilities include: storing names and phone numbers in electronic  
9 "address books;" sending, receiving, and storing text messages and e-mail; taking,  
10 sending, receiving, and storing still photographs and moving video; storing and playing  
11 back audio files; storing dates, appointments, and other information on personal  
12 calendars; and accessing and downloading information from the Internet. Wireless  
13 telephones may also include global positioning system ("GPS") technology for  
14 determining the location of the device.

15           c.     Electronic Storage media: Electronic Storage media is any physical  
16 object upon which computer data can be recorded. Examples include hard disks, RAM,  
17 floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

18           d.     GPS: A GPS navigation device uses the Global Positioning System  
19 to display its current location. It often contains records the locations where it has been.  
20 Some GPS navigation devices can give a user driving or walking directions to another  
21 location. These devices can contain records of the addresses or locations involved in  
22 such navigation. The GPS consists of 24 NAVSTAR satellites orbiting the Earth. Each  
23 satellite contains an extremely accurate clock. Each satellite repeatedly transmits by  
24 radio a mathematical representation of the current time, combined with a special  
25 sequence of numbers. These signals are sent by radio, using specifications that are  
26 publicly available. A GPS antenna on Earth can receive those signals. When a GPS  
27 antenna receives signals from at least four satellites, a computer connected to that antenna  
28 can mathematically calculate the antenna's latitude, longitude, and sometimes altitude



1 with a high level of precision.

2 **FORENSIC ANALYSIS**

3 31. Based on my training, experience, and research, and from consulting with  
4 others, I know that the SUBJECT DEVICES have capabilities that allow them to serve as  
5 electronic storage devices of information and data and, in some cases, instrumentalities of  
6 criminal conduct. For example, a GPS navigation device on the various cell phones  
7 could hold historical information about the device's whereabouts and location searches,  
8 which may serve as evidence and/or assist law enforcement in identifying other co-  
9 conspirators, among other things. The various cell phones may also include records of  
10 communications between and among co-conspirators, including text messages or  
11 voicemails directly regarding the commission of the Target Offenses. And, of course, the  
12 laptop computer, hard drives, and memory cards may hold data relating to gift card  
13 numbers. Finally, in my training and experience, examining data stored on devices of  
14 this type can uncover, among other things, evidence that reveals or suggests who  
15 possessed or used the device.

16 32. Based on my knowledge, training and experience, I know that digital  
17 devices and electronic storage media can store information for long periods of time.  
18 Similarly, things that have been viewed via the Internet are typically stored for some period  
19 of time on the device used to access the Internet. This information can sometimes be  
20 recovered with forensic tools.

21 33. There is probable cause to believe that things that were once stored on the  
22 SUBJECT DEVICES may still be stored there, for at least the following reasons:

23 a. Based on my knowledge, training, and experience, I know that  
24 computer files or remnants of such files can be recovered months or even years after they  
25 have been downloaded onto a digital device or other electronic storage medium, deleted,  
26 or viewed via the Internet. Electronic files downloaded to a digital device or other  
27 electronic storage medium can be stored for years at little or no cost. Even when files  
28 have been deleted, they can be recovered months or years later using forensic tools. This

1 is so because when a person “deletes” a file on a computer, the data contained in the file  
2 does not actually disappear; rather, that data remains on the digital device or other  
3 electronic storage medium until it is overwritten by new data.

4 b. Therefore, deleted files, or remnants of deleted files, may reside in  
5 free space or slack space—that is, in space on the digital device or other electronic  
6 storage medium that is not currently being used by an active file—for long periods of  
7 time before they are overwritten. In addition, a computer’s operating system may also  
8 keep a record of deleted data in a “swap” or “recovery” file.

9 c. Wholly apart from user-generated files, computer storage media—in  
10 particular, computers’ internal hard drives—contain electronic evidence of how a  
11 computer has been used, what it has been used for, and who has used it. To give a few  
12 examples, this forensic evidence can take the form of operating system configurations,  
13 artifacts from operating system or application operation, file system data structures, and  
14 virtual memory “swap” or paging files. Computer users typically do not erase or delete  
15 this evidence, because special software is typically required for that task. However, it is  
16 technically possible to delete this information.

17 d. Similarly, files that have been viewed via the Internet are sometimes  
18 automatically downloaded into a temporary Internet directory or “cache.”

19 34. Forensic evidence. As further described in Attachment B, this application  
20 seeks permission to locate not only ESI that might serve as direct evidence of the crimes  
21 described on the warrant, but also forensic evidence that establishes how the SUBJECT  
22 DEVICES were used, the purpose of its use, who used it, and when. There is probable  
23 cause to believe that this forensic electronic evidence might be on the SUBJECT  
24 DEVICES because:

25 a. Data on a digital device or other electronic storage medium can  
26 provide evidence of a file that was once on the digital device or other electronic storage  
27 medium but has since been deleted or edited, or of a deleted portion of a file (such as a  
28 paragraph that has been deleted from a word processing file). Virtual memory paging

1 systems can leave traces of information on the digital device or other electronic storage  
2 medium that show what tasks and processes were recently active. Web browsers, e-mail  
3 programs, and chat programs store configuration information on the storage medium that  
4 can reveal information such as online nicknames and passwords. Operating systems can  
5 record additional information, such as the attachment of peripherals, the attachment of  
6 USB flash storage devices or other external storage media, and the times the computer  
7 was in use. Computer file systems can record information about the dates files were  
8 created and the sequence in which they were created.

9           b. As explained herein, information stored within a computer and other  
10 electronic storage media may provide crucial evidence of the “who, what, why, when,  
11 where, and how” of the criminal conduct under investigation, thus enabling the United  
12 States to establish and prove each element or alternatively, to exclude the innocent from  
13 further suspicion. In my training and experience, information stored within a computer  
14 or storage media (e.g., registry information, communications, images and movies,  
15 transactional information, records of session times and durations, Internet history, and  
16 anti-virus, spyware, and malware detection programs) can indicate who has used or  
17 controlled the computer or storage media. This “user attribution” evidence is analogous  
18 to the search for “indicia of occupancy” while executing a search warrant at a residence.  
19 The existence or absence of anti-virus, spyware, and malware detection programs may  
20 indicate whether the computer was remotely accessed, thus inculcating or exculpating the  
21 computer owner and/or others with direct physical access to the computer. Further,  
22 computer and storage media activity can indicate how and when the computer or storage  
23 media was accessed or used. For example, as described herein, computers typically  
24 contain information that log: computer user account session times and durations,  
25 computer activity associated with user accounts, electronic storage media that connected  
26 with the computer, and the IP addresses through which the computer accessed networks  
27 and the Internet. Such information allows investigators to understand the chronological  
28 context of computer or electronic storage media access, use, and events relating to the

1 crime under investigation.<sup>4</sup> Additionally, some information stored within a computer or  
2 electronic storage media may provide crucial evidence relating to the physical location of  
3 other evidence and the suspect. For example, images stored on a computer may both  
4 show a particular location and have geolocation information incorporated into its file  
5 data. Such file data typically also contains information indicating when the file or image  
6 was created. The existence of such image files, along with external device connection  
7 logs, may also indicate the presence of additional electronic storage media (e.g., a digital  
8 camera or cellular phone with an incorporated camera). The geographic and timeline  
9 information described herein may either inculcate or exculpate the computer user. Last,  
10 information stored within a computer may provide relevant insight into the computer  
11 user's state of mind as it relates to the offense under investigation. For example,  
12 information within the computer may indicate the owner's motive and intent to commit a  
13 crime (e.g., Internet searches indicating criminal planning), or consciousness of guilt  
14 (e.g., running a "wiping" program to destroy evidence on the computer or password  
15 protecting/encrypting such evidence in an effort to conceal it from law enforcement).

16 c. A person with appropriate familiarity with how a digital device or  
17 other electronic storage medium works may, after examining this forensic evidence in its  
18 proper context, be able to draw conclusions about how the devices were used, the purpose  
19 of their use, who used them, and when.

20 d. The process of identifying the exact electronically stored  
21 information on a digital device or other electronic storage medium that are necessary to  
22 draw an accurate conclusion is a dynamic process. Electronic evidence is not always data  
23 that can be merely reviewed by a review team and passed along to investigators.  
24 Whether data stored on a computer is evidence may depend on other information stored  
25

---

26 <sup>4</sup> For example, if the examination of a computer shows that: a) at 11:00am, someone using the computer  
27 used an internet browser to log into a bank account in the name of John Doe; b) at 11:02am the internet  
28 browser was used to download child pornography; and c) at 11:05 am the internet browser was used to  
log into a social media account in the name of John Doe, an investigator may reasonably draw an  
inference that John Doe downloaded child pornography.

1 on the computer and the application of knowledge about how a computer behaves.  
2 Therefore, contextual information necessary to understand other evidence also falls  
3 within the scope of the warrant.

4 e. Further, in finding evidence of how a device was used, the purpose  
5 of its use, who used it, and when, sometimes it is necessary to establish that a particular  
6 thing is not present on a storage medium.

7 35. Manner of execution. Because this warrant seeks only permission to  
8 examine devices already in law enforcement's possession, the execution of this warrant  
9 does not involve the physical intrusion onto a premises. Consequently, I submit there is  
10 reasonable cause for the Court to authorize execution of the warrant at any time in the  
11 day or night.

12 **DIGITAL DEVICES AS INSTRUMENTALITIES OF THE CRIMES**

13 36. I know that when an individual uses a digital device or other electronic  
14 storage medium to download, store, transfer, or download or upload card data or other  
15 victim-related information, the individual's device will generally serve both as an  
16 instrumentality for committing the crime, and also as a storage medium for evidence of  
17 the crime. The device is an instrumentality of the crime because it is used as a means of  
18 committing the criminal offense. The device is also likely to be a storage medium for  
19 evidence of crime. From my training and experience, I believe that a digital device or  
20 other electronic storage medium used to commit a crime of this type may contain: data  
21 that is evidence of how the device was used; data that was sent or received; and other  
22 records that indicate the nature of the offense.

23 **PRIOR EFFORTS TO OBTAIN EVIDENCE**

24 37. Alternative methods of obtaining the evidence sought after have been  
25 reasonably exhausted. At this time, any other means of obtaining the necessary evidence  
26 could result in an unacceptable risk of the loss/destruction of the evidence sought. Based  
27 on my knowledge, training and experience, the only effective means of collecting and  
28 preserving the required evidence in this case is through a search warrant.

## SEARCH TECHNIQUES

38. Based on the foregoing, and consistent with Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, the warrant I am applying for will permit imaging or otherwise copying all data contained on the SUBJECT DEVICES, and will specifically authorize a review of the media or information consistent with the warrant. The review may require techniques, including computer-assisted scans of the media or information that might expose many parts of the media or information to human inspection in order to determine whether it contains the items described in Attachment B.

39. In accordance with the information in this affidavit, law enforcement personnel will execute the search of the SUBJECT DEVICES pursuant to this warrant as follows:

### **a. Securing the Data**

i. In order to examine the ESI in a forensically sound manner, law enforcement personnel with appropriate expertise will attempt to produce a complete forensic image, if possible and appropriate, of the SUBJECT DEVICES.<sup>5</sup>

ii. A forensic image may be created of either a physical drive or a logical drive. A physical drive is the actual physical hard drive that may be found in a typical computer. When law enforcement creates a forensic image of a physical drive, the image will contain every bit and byte on the physical drive. A logical drive, also known as a partition, is a dedicated area on a physical drive that may have a drive letter assigned (for example the c: and d: drives on a computer that actually contains only one

---

<sup>5</sup> The purpose of using computer personnel to conduct the imaging of digital devices is to ensure the integrity of the evidence and to follow proper, forensically sound, scientific procedures. When the investigative agent is a trained computer examiner, it is not always necessary to separate these duties. Prior to recent court-imposed limitations on the conduct of ESI search warrants, computer personnel typically worked closely with investigative personnel in all investigations involving digital evidence to assist investigators in their search for digital evidence. The point of using computer personnel to segregate data in a digital investigation was typically technological rather than legal. Computer personnel are needed because they generally have technological expertise that investigative agents do not possess. Computer personnel, however, typically lack the factual and investigative expertise that an investigative agent may possess on any given case. Therefore, it is important that computer personnel and investigative personnel work closely together. In more complex computer investigations, especially those involving computer intrusions, law enforcement will often assign an investigative agent with training and experience in computer examinations and/or computer science because of the importance of combining the investigative and technological skills.



1 physical hard drive). Therefore, creating an image of a logical drive does not include  
2 every bit and byte on the physical drive. Law enforcement will only create an image of  
3 physical or logical drives physically present on or within the SUBJECT DEVICES.  
4 Creating an image of the SUBJECT DEVICES will not result in access to any data  
5 physically located elsewhere. However, SUBJECT DEVICES that have previously  
6 connected to devices at other locations may contain data from those other locations.

7 **b. Searching the Forensic Images**

8 i. Searching the forensic images for the items described in  
9 Attachment B may require a range of data analysis techniques. In some cases, it is  
10 possible for agents and analysts to conduct carefully targeted searches that can locate  
11 evidence without requiring a time-consuming manual search through unrelated materials  
12 that may be commingled with criminal evidence. In other cases, however, such  
13 techniques may not yield the evidence described in the warrant, and law enforcement  
14 may need to conduct more extensive searches to locate evidence that falls within the  
15 scope of the warrant. The search techniques that will be used will be only those  
16 methodologies, techniques and protocols as may reasonably be expected to find, identify,  
17 segregate and/or duplicate the items authorized to be seized pursuant to Attachment B to  
18 this affidavit.

19 ii. The search techniques that will be used will be only those  
20 methodologies, techniques and protocols as may reasonably be expected to find, identify,  
21 segregate and/or duplicate the items authorized to be seized pursuant to Attachment B to  
22 this affidavit. These methodologies, techniques and protocols may or may not include  
23 the use of a "hash value" library to exclude normal operating system files that do not  
24 need to be further searched. Or, agents may utilize hash values to exclude certain known  
25 files, such as the operating system and other routine software, from the search results.  
26 However, because the evidence I am seeking does not have particular known hash values,  
27 agents will not be able to use any type of hash value library to locate the items identified  
28 in Attachment B.

1       40. Manner of execution. Because this warrant seeks only permission to  
2 examine devices already in law enforcement's possession, the execution of this warrant  
3 does not involve the physical intrusion onto a premises. Consequently, I submit there is  
4 reasonable cause for the Court to authorize execution of the warrant at any time in the  
5 day or night.

6                                   **REQUEST FOR SEALING**

7       41. It is respectfully requested that this Court issue an order sealing all papers  
8 submitted in support of this application, including the application and search warrant. I  
9 believe that sealing this document is necessary because the warrant is relevant to an  
10 ongoing investigation into criminal organizations and not all of the targets of this  
11 investigation, including several persons identified herein, will be searched at this time.  
12 Based upon my training and experience, I have learned that, some criminals actively  
13 search for criminal affidavits and search warrants via the internet, and disseminate them  
14 to other others as they deem appropriate, i.e., post them publicly online through the  
15 carding forums. This is of particular importance here, where the criminal conspiracy at  
16 issue involves numerous persons, many who remain unidentified, and conduct outside the  
17 United States. Moreover, the investigation has utilized and continues to utilize  
18 cooperating co-conspirators. Premature disclosure of the contents of this affidavit and  
19 related documents may have a significant and negative impact on the continuing  
20 investigation and may severely jeopardize its effectiveness.

21                                   **CONCLUSION**

22       42. Based on the foregoing, I believe there is probable cause that evidence,  
23 fruits, and instrumentalities of violations of 18 U.S.C. §§ 371 and 1349 (Conspiracy), 18  
24 U.S.C. § 1029 (Access Device Fraud), and 18 U.S.C. § 1343 (Wire Fraud), are located in  
25 the SUBJECT DEVICES, as more fully described in Attachment A to this Affidavit. I


26 //

27 //

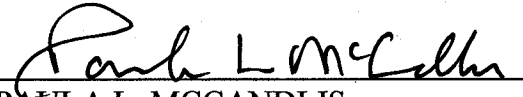
28 //



1 therefore request that the court issue a warrant authorizing a search of the SUBJECT  
2 DEVICES for the items more fully described in Attachment B hereto, incorporated herein  
3 by reference, and the seizure of any such items found therein.  
4

5  
6   
7 YOSHIKO MARINKO, Affiant  
8 Special Agent  
9 United States Secret Service

10 The above-named agent provided a sworn statement attesting to the truth of the  
11 contents of the foregoing affidavit on 4 day of August, 2018.  
12

13  
14   
15 PAULA L. MCCANDLIS  
16 United States Magistrate Judge  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

**ATTACHMENT A**

**SUBJECT DEVICES TO BE SEARCHED**

- (a) Lenovo Laptop, Black; Serial # CB18751780; Model G585
- (b) Acer Laptop, Black; Serial # NXGFTAA0117020D2253400; Model # N16C1
- (c) Moto Cell Phone; Model XT1687; Serial # Inaccessible
- (d) Huawei Honor Cell Phone; Model BLN-L24; Serial # Inaccessible
- (e) Sandisk Flash Drive, 32 GB; BM170525665Z
- (f) Transcend Flash Drive, 4GB; N14939
- (g) Samsung Galaxy S9+ phone, Black; Serial # R38K30T7Q2Z; IMEI:  
343321092412611

All of the aforementioned items or devices are currently in the custody of the  
United States Secret Service, located in Seattle, Washington

**ATTACHMENT B**  
**ITEMS TO BE SEIZED**

All evidence on the SUBJECT DEVICES described in Attachment A that constitutes fruits, contraband, evidence and instrumentalities of violations of 18 U.S.C. §§ 371 and 1349 (Conspiracy), 18 U.S.C. § 1029 (Access Device Fraud), 18 U.S.C. § 1343 (Wire Fraud) (collectively, the "Subject Offenses"), for the time period of **January 1, 2017 to December 1, 2017**, including:

a. Documents, records or files relating to the identification of the individuals committing the Subject Offenses

b. Documents, records or files relating to credit/debit card, gift card, or account or card numbers;

c. Documents, records or files relating to planned, attempted, or successful use of gift cards or card data to conduct purchases or transactions;

d. Documents, records or files relating to the purchase, receipt, manufacture, maintenance, or use of card-reading or encoding equipment or software, device-making equipment;

e. Documents, records or files relating to the creation, manufacture, possession, transfer, or use of counterfeit cards or stolen card data, including the Luhn algorithm software or files that may be used for encoding and/or re-encoding gift cards;

f. Documents, records or files relating to or referencing Target, transactions conducted at Target, items or services purchased from Target, or communications about Target or with Target representatives;

g. Documents, records or files relating to online vendors, such as Paxful, where gift cards and gift card balances may be listed, sold, or purchased;

h. Documents, records or files relating to cryptocurrency, such as Bitcoin, and the use and possession thereof, including any wallets and passcodes and public/private keys thereto;

i. Documents, records or files indicating dominion and control;

1 j. Documents, records or files relating to the deposit, withdrawal, or transfer  
2 of funds, including, but not limited to, wire transfers;

3 k. Photographs depicting cash, cards/card stock, device-making equipment,  
4 transactions, and/or any other individual that may be involved in the criminal scheme;

5 l. Documents, records or files establishing criminal associations, including  
6 address books, contact lists, and telephone or communication records;

7 m. Documents, records or files relating to software, programs or applications,  
8 such as Pocket Zee, that enables the use of gift cards or gift card numbers on digital  
9 devices;

10 n. Documents, records or files relating to the use or sale of items purchased  
11 using stolen Target gift card numbers;

12 o. Evidence of user attribution showing who used or owned the SUBJECT  
13 DEVICES at the time the things described in this warrant were created, edited, or deleted,  
14 such as logs, phonebooks, contact lists, saved usernames and passwords, documents,  
15 pictures/photographs, and browsing history;

16 p. Records and/or data that may reveal the past location of the individual or  
17 individuals using the SUBJECT DEVICES;

18 q. Any passwords, password files, test keys, encryption codes or other  
19 information necessary to access computer equipment, storage devices or data.

20 r. For each of the SUBJECT DEVICES:

21 i. Evidence of who used, owned, or controlled the digital device or  
22 other electronic storage media at the time the things described in this warrant were  
23 created, edited, or deleted, such as logs, registry entries, configuration files, saved  
24 usernames and passwords, documents, browsing history, user profiles, email, email  
25 contacts, "chat," instant messaging logs, photographs, and correspondence;

26 ii. Evidence of software that would allow others to control the digital  
27 device or other electronic storage media, such as viruses, Trojan horses, and other forms  
28

1 of malicious software, as well as evidence of the presence or absence of security software  
2 designed to detect malicious software;

3           iii.       Evidence of the lack of such malicious software;

4           iv.       Evidence of the attachment to the digital device of other storage  
5 devices or similar containers for electronic evidence;

6           v.       Evidence of counter-forensic programs (and associated data) that are  
7 designed to eliminate data from the digital device or other electronic storage media;

8           vi.       Evidence of the times the digital device or other electronic storage  
9 media was used;

10          vii.       Passwords, encryption keys, and other access devices that may be  
11 necessary to access the digital device or other electronic storage media;

12          viii.       Documentation and manuals that may be necessary to access the  
13 digital device or other electronic storage media or to conduct a forensic examination of  
14 the digital device or other electronic storage media;

15          ix.       Contextual information necessary to understand the evidence  
16 described in this attachment.

17  
18  
19       As used above, the terms “documents,” “records,” and “information” include all of  
20 the foregoing items of evidence in whatever form and by whatever means they may have  
21 been created or stored, including any form of computer or electronic storage (such as  
22 flash memory or other media that can store data) and any photographic form.  
23  
24  
25  
26  
27  
28